Top 10 Findings

The following Top 10 Findings are based on the high level results of the 2006 Employer Information Security Survey, completed in January 2007. The survey represents the responses of 261 Information Security professionals (representing 261 Southeast Michigan companies). A more in-depth view can be found in the report.

1. There is a strong awareness of, and commitment for the issue of addressing Information Security within respondents' respective companies. The majority of those responding to this question agreed that *Information Security* is a high priority in their company, with one-third anticipating a strong increase in focus.

2. While the industry sectors of Government, Information, Finance and Health Services are the most aggressive in their anticipated focus on *information security,* Manufacturing appears to be the least aggressive with the majority anticipating only a "moderate increase" in the focus on Information Security. In terms of current budget allocations, Manufacturing also currently spends the least of any industry on personnel and training.

3. In terms of what companies are actually doing in this area, the data reveals a strong polarization between "focus" and actual implementation. One in two companies currently spends less than 10% of their budget on Information Security personnel or training. This is confirmed by a national study (Accenture/IDC) which had almost identical findings from their survey among CIO's and CSO's of U.S. corporations.

4. This polarization is also reflected by the geographic span of a companies' business. While over 90% of respondents from companies with global operations currently hold some type of Information Security degree or certification, less than one in four companies with local to U.S. market presence can also claim this level of Information Security training or education. This becomes particularly alarming when one considers that the Internet as a primary channel of communication is no less of a threat among local businesses than global businesses. Suppliers to global companies not only put themselves at risk, but by their vendor relationship can also subject large global corporations to third party breaches. The SANS Institute report on "The Ten most Important Security Threats of the Coming Year" completed in 2006 underlines this unsettling situation by revealing "mobile devices" (laptops, PDAs, smart phone and other wireless communications) as the number one threat. The rapid pace of business and the increasing need for companies to communicate, and collaborate with vendors or suppliers in a cyberspace environment facilitated by Internet, wireless and mobile devices highlights the risk.

5. To date, typical information security initiatives could be classified as *reactive* in nature. "Business continuity," "disaster recovery," "identity and access management," and "intrusion prevention systems" have been the primary areas of focus with many of these initiatives driven by government regulations such as Sarbanes Oxley.

6. However, it appears that the opportunity for *proactive* initiatives is going to expand very rapidly over the next few years. Companies are anticipating increased budget commitments for personnel and training being led at this point by information sensitive industries such as Finance, Information and Professional Business Services. Companies with global operations are being driven not only by required adherence to government requirements (i.e., Sarbanes Oxley) but also by strategic need; to protect their competitive assets (i.e., corporate plans, knowledge, skills, R&D).

7. Salary expectations of information technology positions are in-line with forecasts from the Michigan Department of Labor and Economic Growth through 2012.

8. Supporting this view of proactive focus, when asked what they consider to be the "Top 5 new frontiers for information security," respondents identified the top 2 initiatives as *Information Risk Management, Security Management Practices.* However companies still tend to regard Information Security as an individual company responsibility. Adherence to industry standards such as ISO 27001 (Information Security Management Systems) or ISO/IEC 27002 (Code of Practice for IS managers) fell to the bottom in terms of "new frontiers."

9. There is still strong fragmentation in terms of educational requirements for positions in Information Security. Traditional careers in information technology, a natural conduit for Information Security, have set the minimums as typical degrees required for those positions. However, as global initiatives take place (GAISP) to formalize standards and practices for careers in "Information Security," educational requirements will become more defined. The best example is Data Administration careers which typically have not required a degree, however in the future respondents anticipate will require "certification" in Information Security.

10. The issue of "certification" is also still very fragmented. Stated requirements of certification for Information Security personnel is still primarily only a requirement among companies with global operations and has yet to trickle down to companies who describe themselves as national, regional or local in business. Awareness of where to get certifications and types of certifications available is very fragmented driven primarily by companies whose software and technology tools are being put in place for Information Security purposes such as CISCO.